Privacy Statement on the Protection of Personal Data in relation to the Internal Audit process

1. Introduction

The Single Resolution Board (hereafter 'SRB') is committed to protect your personal data and to respect your privacy. The SRB Internal Audit collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001) (EUDPR).

This privacy statement of the SRB Internal Audit (IA) explains the reason for the processing of your personal data, the way the IA collects, handles and ensures protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

2. Why and how do we process your personal data?

The SRB IA collects and uses your personal data to conduct internal audit activities in accordance with Articles 74 and 75 of SRB 'Financial Regulation'(Regulation lay down by SRB PS Decision SRB/ PS/2020/05) or the respective applicable legal framework as indicated in section 4 "Authority" of the Internal Audit mission charter. In this respect, the IA enjoys complete independence and full and unlimited access to all information required to perform its duties in relation to all the activities and departments of the SRB.

We advise SRB departments on how to deal with risks, by issuing objective opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management. We therefore interview staff responsible for these operations, analyse underlying documentation (internal guidance, checklists, payments made, etc.) and transactions in information systems and assess the operation of the internal controls put in place by management in respect of these operations.

Therefore, the internal audit activities do not typically target natural persons as such. Nevertheless, during the course of our activities, personal data within the meaning of Article 3(1) EUDPR are inevitably processed. Your personal data will not be used for an automated decision-making including profiling.

3. On what legal ground(s) do we process your personal data

The legal bases for processing your personal data are the following:

- Article 5(1)(a) and Recital 22 of EUDPR: processing is necessary for the performance of a task carried out in the public interest by the SRB (which is the proper management and functioning of the SRB).
- Article 5(1)(b) of EUDPR: processing is necessary for compliance with a legal obligation to which the controller is subject:
    - Article 62 of Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit

institutions and certain investment firms in the framework of a SingleResolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010 (SRMR);

- Articles 74 and 75 of SRB 'Financial Regulation';
- SRB Internal audit charter.

In the course of its audit activities, the SRB IA may process special categories of personal data, pursuant to Article 10 of EUDPR, or personal data related to criminal convictions and offences, pursuant to Article 11 of EUDPR, only if necessary for a task carried out in the public interest and to comply with the legal obligations to which the IA is subject. As such, the IA may process, for example, data required prior to recruitment such as data concerning health or criminal record in the context of an audit on recruitment by the SRB.

The processing of such data will not constitute the major aim of the engagement, as the internal audit activities do not aim at investigating/inquiring particular individuals and/or conduct. In addition, the processing of the data falls within the reasonable expectations of data subjects, based on their relationship with the IA (a candidate participating in a recruitment procedure in SRB can expect that an SRB Internal Audit on the recruitment process may involve the processing of his or her personal data). Furthermore, the risks to the fundamental rights and freedoms of data subjects, related to the processing of special categories personal data do not relate to the internal audit process, but to the activities for which they were initially collected (personal data available in recruitment files may be accessed by the IA, but the IA has no influence over the purpose and means of the initial processing).

4. Which personal data do we collect and further process?

In performing its internal audit activities, the SRB IA collects the following categories of personal data: identification data, contact data, professional data and data related to or brought in connection with the subject matter of the activity, special categories of personal data.

Your personal data may be obtained during our audit activities from documents we analyse in the course of our engagements (minutes of meetings, transactions in information systems, operational instructions given by or on behalf of the auditee or other types of data specific to the engagement, etc.).

5. How long do we keep your personal data?

The IA only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for compliance with our legal obligations under the Financial Regulation of the Single Resolution Board (SRB/ PS/2020/05) The IA adheres to the SRB policy on records management1 for electronic archiving and document management. The administrative retention period for internal audit reports is 10 years. Audit documents and records (e.g. audit working papers) are kept for six years.

At the end of the administrative retention period, the files related to the internal audit activity (including personal data) are transferred to the historical archives of the SRB (in the case of audit reports) or destroyed (in the case of supporting documents, e.g. audit working papers).

6. How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the SRB. All processing operations are carried out pursuant to the SRB's ICT security policies, on the security of communication and information systems in the SRB.

In order to protect your personal data, the SRB has put in place a number of technical and organisational measures. **Technical measures** include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. **Organisational measures** include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation. In addition, all IA audit staff have received the appropriate briefing on the legal provisions of EUDPR and are expected to respect the code of ethics of the Institute of Internal Auditors, which requires internal auditors to, inter alia, be prudent in the use and protection of information acquired in the course of their duties.

7. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the SRB staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The output of the internal audit work is an engagement report which is delivered to the head of the entity audited (e.g. SRB Chair and relevant Directors as well as to the Executive Session).

Copies are made available to:

- The SRB Chair, RMIC (Risk Management and Internal Control) function /Internal Control Coordinator(s) and other services responsible for the implementation of the recommendations; • the SRB Executive Session;
- the European Court of Auditors;
- OLAF, in exceptional cases where there is a suspicion of fraud or indications or findings related to systemic weaknesses or individual situations that show a potential vulnerability, in line with the administrative arrangements between the SRB and OLAF;
- Further transmission of the report by the auditee within his own department is decided by the head of the organisational entity.

The working papers containing audit evidence are not transmitted.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law or base on a contractual agreement.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of EUDPR, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

9. Contact information

- The Data Controller: If you would like to exercise your rights under EUDPR, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Internal Audit team at: SRB-InternalAudit@srb.europa.eu.
- The Data Protection Officer (DPO) of the SRB You may contact the Data Protection Officer (SRB-DPO@srb.europa.eu) with regard to issues related to the processing of your personal data under EUDPR.
- The European Data Protection Supervisor (EDPS) You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under EUDPR have been infringed as a result of the processing of your personal data by the Data Controller

10. Where to find more detailed information?

The SRB keeps the Public register of all processing operations on personal data (public register) , which have been documented and notified. You may access the public register here.

This specific processing operation has been included in the SRB's public register.